UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/670,298	09/26/2003	Andrea Klaes	SRE0003-US	6494

7590 11/17/2006

Michael D. Bednarek
SHAW PITTMAN LLP
1650 TYSONS BOULEVARD
MCLEAN, VA 22102

EXAMINER	
SHAN, APRIL YING	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/670,298	KLAES, ANDREA	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 September 2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 have been examined.

Admitted Prior Art

2. Examiner is aware of Admitted Prior Art in the Applicant's specification, line 6 of paragraph [0030], on page 9 - line 2 on page 10.

Priority

3. Examiner is aware of the application claims priority of U.S. Provisional Application No. 60/413,763, filed on September 27, 2002.

Drawings

4. The drawings are objected to because the word "network" is not showing on Fig. 1, element 150. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the

examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

5. Claim 19 is objected to because of the following informalities:

a. "The system of claim 1, wherein..." should be "The system of claim 12, wherein..." in claim 19;

Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-30 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

In claims 1-11, a "system" is being recited; however, it appears that the system would reasonably be interpreted by one of ordinary skill in the art as software, per se. On page 5, par. [0017] of the specification, the Applicant defined "both proxy and central loghosts are independent modules". Also, on page 4, par. [0015] of the specification, the Applicant defined "resources" is to be constructed broadly as "any system that may be connected to (or operating within) a given network and that generates log

files....many enterprise software applications...and the like generate log files....". All other claim limitations such as software adapters, module, log files are software. As such, it believes that the system of claims 1-11 are reasonably interpreted as functional descriptive material, per se.

In claims 12-21, a "system" is being recited; however, it appears that the system would reasonably be interpreted by one of ordinary skill in the art as software, per se. On page 5, par. [0017] of the specification, the Applicant defined "both proxy and central loghosts are independent modules". Also, on page 4, par. [0015] of the specification, the Applicant defined "resources" is to be constructed broadly as "any system that may be connected to (or operating within) a given network and that generates log files....many enterprise software applications...and the like generate log files....". All other claim limitations such as software adapters, module, log files are software. As such, it believes that the system of claims 12-21 are reasonably interpreted as functional descriptive material, per se.

In claims 22-30, a "method" is being recited. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. The claimed steps do not result in a tangible result. Claims 22-30 are rejected as being directed to an abstract idea (i.e., producing non-tangible result) [tangible requirement does require that the claim must recite more than a 101 judicial exception, in that the process must set forth a practical application of that 101 judicial exception to produce a real-world result, Benson, 409 U.S. at 71-72, 175 USPQ at 676-77).

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-7, 9-17, 19-28 and 30 are rejected under 35 U.S.C. 102(e) as being anticipated by Khanolkar et al. (U.S. Patent No. 7,127,743)

As per **claim 1**, Khanolkar et al. discloses a monitoring/intrusion detection system (e.g. abstract), comprising:

a central loghost ("an event manager" disclosed in the abstract corresponds to Applicant's central loghost),

at least one proxy loghost ("syslog listener and an event parser" disclosed in col. 7, lines 45-46 corresponds to Applicant's proxy loghost) in communication with the central loghost; and

at least one monitoring station ("event broadcaster 56" in fig. 2 corresponds to one monitoring station),

wherein the proxy loghost receives a plurality of log files (log data 18 in fig 1) from a plurality of resources (e.g. col. 3, lines 59- col. 4, line 2) operating on a network, analyzes the log files for at least one of unexpected volume, unexpected patterns ("a

developing pattern of intrusion" – e.g. col. 4, lines 54-55. Please note the word "intrusion" should be broadly understood to include any type of security breach and accidental or inadvertent misuse as well as an actual intrusion disclosed in col. 3, lines 5-9. Therefore, it meets the claim limitation of unexpected patterns) or unexpected types of log files, and generates events in view of such analysis (col. 7, lines 47-53),

wherein the central loghost is operable to receive the events generated by the proxy loghost and generate an alert upon an analysis of the events, and wherein the monitoring station is caused to issue an alarm when the alert is generated (col. 7, lines 14-22 and col. 7, line 53 – col. 8, line 11)

Please also note on col. 2, lines 25-44, Khanolkar et al. discloses "the system has discrete software modules that receive and process log data from various network devices....". In light of the Applicant's specification in paragraph [0017] that both proxy and central loghosts are independent modules and they can run on the same system. Therefore, the teachings of Khanolkar et al. met the limitations of the claim.

As per **claim 2**, Khanolkar et al. discloses a system as applied in claim 1. Khanolkar et al. further discloses wherein the central loghost comprises a plurality modules operating in a Unix environment ("system 10 is preferably...implemented on ...Linux or Solaris server platforms..." –e.g. col. 4, lines 11-12).

Please note Linux is unix-like operating system and has unix background. Therefore, it met the limitation of the claim.

As per **claim 3**, Khanolkar et al. discloses a system as applied in claim 1. Khanolkar et al. further discloses comprising a plurality of proxy loghosts, each one of the plurality being in communication with the central loghost ("an event manager in communication with the event parser" – e.g. abstract and "a plurality of event parsers" – e.g. col. 7, lines 46—54).

As per **claim 4**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein the resources comprise at least one of an operating system, application, firewall, router, switch and loadbalancer (e.g. col. 3, lines 59 – col. 4, line 1).

As per **claim 5**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein a plurality of events is required to cause the generation of an alert ("It is also contemplated that a user may set no threshold...and allow the generation of alarms and broadcast of all event objects received at 160" – e.g. col. 7, line 60- col. 8, line 3)

As per **claim 6**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. met the limitation of claim 6 by further disclose wherein security management has access to both the proxy loghost and the central loghost ("....In event manager 55, as well as in other system modules and features, filter settings may be set by a user, for instance, a network administrator through web client interface

30...Settings may be modified by a user during system 10 operation by further input into web client interface 30" – e.g. col. 6, lines 38-54)

As per **claim 7**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein the log files are received from a network-based intrusion detection system (e.g. col. 2, lines 1-9)

As per **claim 9**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein the log files are archived on the proxy loghost and the events are archived on the central loghost (col. 1, lines 54- 62, col. 7, lines 24-29 and col. 7, lines 24-31).

Please note that proxy loghost and central loghost are running on the system 10 of the Khanolkar et al. And the database to hold archived files are located in the database 58 within the system 10 in fig. 2. Therefore, the teaching of Khanolkar et al. met the limitation of the claim.

As per **claim 10**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses comprising software adapters to convert one format of a log file to another format ("...log data...are converted to event objects for processing and manipulation by the system..." –e.g. col. 2, lines 25-32).

As per **claim 11**, Khanolkar et al. discloses the system as applied in claim 1. Khanolkar et al. further discloses comprising a module for visualizing the log files received at the proxy loghost ("system 10 operates in conjunction with a web server, such as Apache or Netscape" – e.g. col. 4, lines 14-15).

As per **claims 12 and 22**, Khanolkar et al. discloses a system/method, comprising:

a plurality of proxy loghosts ("discrete software modules" – e.g. col. 2, line 25), each proxy loghost collecting log files that are generated by resources in a portion of the secure network, the plurality of loghosts generating events in response to the log files collected (e.g. col. 2, lines 28-32); and

a central loghost in communication with the plurality of proxy loghosts, the central loghost receiving at least one of (i) the log files themselves and (ii) the events from the plurality of proxy loghosts (Examiner's interpretation on the limitation is that receiving at least one of the log files themselves or the events from the plurality of proxy loghosts), the central loghost analyzing the events to determine the necessity of generating an alert and an associated alarm to notify (col. 7, lines 14-22 and col. 7, line 53 – col. 8, line 11) a security manager ("a network security administrator or other network administrator" in col. 4, lines 44-45 corresponds to Applicant's security manager) of a possible intrusion incident.

As per **claims 13 and 23**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the central loghost comprises a plurality modules operating in a Unix environment ("system 10 is preferably... implemented on ... Linux or Solaris server platforms..." –e.g. col. 4, lines 11-12).

As per **claims 14 and 25**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the resources comprise at least one of an operating system, application, firewall, router, switch and loadbalancer (e.g. col. 3, lines 59 – col. 4, line 1).

As per **claim 15**, Khanolkar et al. discloses a system as applied in claim 12. Khanolkar et al. further discloses wherein a plurality of events is required to cause the generation of an alert ("It is also contemplated that a user may set no threshold... and allow the generation of alarms and broadcast of all event objects received at 160" – e.g. col. 7, line 60- col. 8, line 3).

As per **claims 16 and 27**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein security management has access to both the plurality of proxy loghosts and the central loghost ("....In event manager 55, as well as in other system modules and features, filter settings may be set by a user, for instance, a network administrator through web client interface

30...Settings may be modified by a user during system 10 operation by further input into web client interface 30" – e.g. col. 6, lines 38-54)

As per **claims 17 and 28**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the log files are received from a network-based intrusion detection system (e.g. col. 2, lines 1-9)

As per **claims 19 and 30**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the log files are archived on the plurality of proxy loghosts and events are archived on the central loghost (col. 1, lines 54- 62, col. 7, lines 24-29 and col. 7, lines 24-31).

Please note that proxy loghost and central loghost are running on the system 10 of the Khanolkar et al. And the database to hold archived files are located in the database 58 within the system 10 in fig. 2. Therefore, the teaching of Khanolkar et al. met the limitation of the claim.

As per **claim 20**, Khanolkar et al. discloses the system as applied in claim 12. Khanolkar et al. further discloses comprising software adapters to convert one format of a log file to another format ("...log data...are converted to event objects for processing and manipulation by the system..." –e.g. col. 2, lines 25-32).

As per **claim 21**, Khanolkar et al. discloses the system as applied in claim 12. Khanolkar et al. further discloses comprising a module for visualizing the log files received at the proxy loghost ("system 10 operates in conjunction with a web server, such as Apache or Netscape" – e.g. col. 4, lines 14-15).

As per **claim 24**, Khanolkar et al. discloses the method as applied in claim 22. Khanolkar et al. further discloses wherein a plurality of proxy loghosts receive log files (col. 7, lines 38-50).

As per **claim 26**, Khanolkar et al. discloses the method as applied in claim 22. Khanolkar et al. further discloses comprising generating the alert only after a plurality events are received ("Therefore, the determination of whether to broadcast the event object as an intrusion alarm is made nearly instantaneously upon receipt of the event object" – e.g. col. 7, lines 14-22 and "It is also contemplated that a user may set no threshold...and allow the generation of alarms and broadcast of all event objects received at 160" – e.g. col. 7, line 60- col. 8, line 3).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

12. Claims 8, 18 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanolkar et al. as applied to claims 1-7, 9-17, 19-28 and 30 above, and further in view of Admitted prior art disclosed on line 6 of paragraph [0030], on page 9 - line 2 on page 10 of the specification of the current application.

As per **claim 8**, Khanolkar et al. discloses the limitation in claim 1 above and also in col. 1, line 23, Khanolkar discloses "password attacks", which is a type of attack Host-based intrusion system usually detects. Khanolkar et al. is silent on wherein the log files are received from a host-based intrusion detection system. However, such missing feature in Khanolkar et al. is clearly taught as Admitted prior art on line 6 of paragraph [0030], on page 9 - line 2 on page 10 of the aforementioned Applicant's specification, the same field endeavor. It would have been obvious for a person having ordinary skill in the art to incorporate such well known feature as taught in the Applicant's admitted prior art into Khanolkar et al.'s system motivated by monitoring and analysis on the internals of a computing system to avoid attacks such as password attacks.

As per **claims 18 and 29**, Khanolkar et al. discloses a system/method as applied in claims 12 and 22 and also in col. 1, line 23, Khanolkar discloses "password attacks", which is a type of attack Host-based intrusion system usually detects. Khanolkar et al. is silent on wherein the log files are received from a host-based intrusion detection system. However, such missing feature in Khanolkar et al. is clearly taught as Admitted prior art on line 6 of paragraph [0030], on page 9 - line 2 on page 10 of the aforementioned Applicant's specification, the same field endeavor. It would have been obvious for a person having ordinary skill in the art to incorporate such well known feature as taught in the Applicant's admitted prior art into Khanolkar et al.'s system motivated by monitoring and analysis on the internals of a computing system to avoid attacks such as password attacks.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Sherlock et al. (U.S. Pub. No. 2002/0093527) discloses a user interface for a network security policy monitoring network.
- Campbell et al. (U.S. Patent No. 6,839,850) discloses a Security Indications and Warning Engine usable in conjunction with an audit agent.
- Holloway et al. (U.S. Patent No. 5,805,801) discloses a system and method for providing security against intrusion in a campus LAN network.
- Hodges (U.S. Pub No. 2002/0112185) discloses a system that can be used to monitor for an attempted intrusion of an access system.

- Connary et al. (U.S. Pub No. 2004/0044912) discloses a network device such as intrusion detection systems.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

2 November 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100